

IN THE UNITED STATES DISTRICT COURT
FOR THE WESTERN DISTRICT OF NORTH CAROLINA
CHARLOTTE DIVISION

IN THE MATTER OF THE SEARCH OF
INFORMATION ASSOCIATED WITH
EMAIL ADDRESS
shadab.siddiqui@gmail.com
THAT IS STORED AT PREMISES
CONTROLLED BY GOOGLE LLC

Case No. 3:20-mj-137

Filed Under Seal

**AFFIDAVIT IN SUPPORT OF
AN APPLICATION FOR A SEARCH WARRANT**

I, Special Agent Brittany M. Wright, with the United States Secret Service,
Charlotte Field Office, being duly sworn, state as follows:

INTRODUCTION AND AGENT BACKGROUND

1. I make this affidavit in support of an application for a search warrant for information associated with a certain account, **shadab.siddiqui@gmail.com**, that is stored at premises controlled by Google LLC, hereinafter “GOOGLE,” a multinational technology company and email provider headquartered in Mountain View, California. The information to be searched is described in the following paragraphs and in Attachment A. This Affidavit is made in support of an application for a search warrant under 18 U.S.C. §§ 2703(a), 2703(b)(1)(A) and 2703(c)(1)(A) to require GOOGLE to disclose to the government copies of the information (including the content of communications) further described in Section I of Attachment B. Upon receipt of the information described in Section I of Attachment B, government-authorized persons will review that information to locate the items described in Section II of Attachment B.

2. I am a Special Agent with the United States Secret Service and have been so employed since May 2019. I am therefore an "investigative or law enforcement officer" of the United States within the meaning of Title 18 United States Code, Section 2510(7). I am empowered by law to conduct investigations and to make arrests and seize assets for federal felony violations. I have been part of investigations involving bank fraud, wire fraud and identify fraud. Prior to becoming a Special Agent, I was a contracted Asset Forfeiture Data Analyst with the United States Attorney's Office for the Western District of Virginia and the Drug Enforcement Administration in Roanoke, Virginia.

3. This Affidavit is intended to show merely that there is sufficient probable cause for the requested warrant and does not set forth all of my knowledge about this matter.

4. Based on my training and experience and the facts as set forth in this Affidavit, there is probable cause to believe that violations of 18 U.S.C. § 2314 (Interstate Transportation of Stolen Property), 18 U.S.C. § 371 (Conspiracy), and 18 U.S.C. §§ 1956 and 1957 (Money Laundering) have been committed by Shadab Siddiqui, hereinafter "SIDDIQUI." There is also probable cause to search SIDDIQUI's email account, **shadab.siddiqui@gmail.com**, for evidence of these crimes further described in Attachment B.

JURISDICTION

5. This Court has jurisdiction to issue the requested Warrant because it is "a court of competent jurisdiction" as defined by 18 U.S.C. § 2711. 18 U.S.C. §§ 2703(a), (b)(1)(A), & (c)(1)(A). Specifically, the Court is "a district court of the United States . . . that has jurisdiction over the offense being investigated." 18 U.S.C. § 2711(3)(A)(i).

PROBABLE CAUSE

Background of Siddiqui's eBay Scheme

6. In January 2020, the Charlotte-Mecklenburg Police Department (CMPD) and United States Secret Service opened an investigation into Shadab SIDDIQUI, for a scheme in which SIDDIQUI buys brand new, in-box items such as vacuum cleaners, from individuals who stole the items from retail stores located in the Charlotte metropolitan area. As part of the scheme, SIDDIQUI then sells the stolen items at below-retail prices on his personal eBay account.

7. According to subpoenaed documents received by your Affiant from eBay, SIDDIQUI (named as “Shadab SIDDIQUI” in eBay documents) opened eBay store “sidd_2400,” hereinafter “the EBAY STORE,” on or about August 23, 2005. On or about October 31, 2017, the EBAY STORE’S physical address was changed to 2400 Maple Grove Lane, NW, Concord, North Carolina, hereinafter “the PREMISES”¹ by someone with access to the EBAY STORE account. The PREMISES is also listed as the shipping address for the EBAY STORE, and **shadab.siddiqui@gmail.com**, hereinafter “the EMAIL ACCOUNT,” is the EBAY STORE’s email address. Between approximately January 1, 2019, and March 9, 2020 (approximately fifteen months), approximately 1,500 items were listed in and subsequently sold for approximately \$330,000.00. The overwhelming majority of those items had sales titles that included the word “new,” and almost all of the items were shipped outside North Carolina. Approximately 75% of those items were listed for sale from SIDDIQUI’S home IP address at the

¹ The United State is simultaneously seeking a search warrant in the Middle District of North Carolina for the PREMISES.

PREMISES.² As of May 18, 2020, the EBAY STORE has approximately forty-nine (49) unique items listed for sale. All but two (2) items are described as “new,” and the only used items are refrigerator shelves.

8. Your Affiant knows that items advertised on eBay’s website must be listed by a person using an electronic device capable of connecting to the Internet. Therefore, when items were listed for sale in the EBAY STORE, someone must have connected an electronic device, such as a smart mobile phone, a tablet, or computer, to the Internet using an IP address in order to list the item on eBay’s website.

Interview with Co-Conspirator

9. On or about January 9, 2020, J.S. was interviewed by Charlotte-Mecklenburg Police Detectives in Charlotte, North Carolina after being arrested for being in possession of a stolen vehicle. J.S., a state-convicted felon for larceny, advised that J.S. used to sell stolen brand new-in-box items to “Tool King” (a Charlotte, North Carolina store that was the subject of a 2018 Interstate Transportation of Stolen Property investigation that resulted in the seizure of more than \$1,000,000.00 in stolen new-in-box items in late 2018 by the Charlotte-Mecklenburg Police Department and United States Secret Service).

10. J.S. admitted to currently selling “most of my stuff [stolen new-in-box items] to” an Indian male that J.S. knows as “SIDD.” J.S. advised that he first met “SIDD” after advertising for sale a new-in-box stolen item on an internet marketplace named “OfferUp.” According to

² According to subpoenaed documents received by your Affiant from Charter Communications, IP address 75.178.132.20 was issued to “Shadab SIDDIQUI” at the PREMISES.

J.S., “SIDD” offered to purchase more items from J.S., and as a result of their initial meeting, J.S. admitted to continuing to steal new-in-box items from retail stores in Charlotte, North Carolina and specifically that he steals items that “sell the best.” J.S. stated that “SIDD” does “not really order up [specific items] but just what resells; resells like on eBay.” According to J.S., “SIDD” is always “by himself” and that before J.S. meets “SIDD,” “SIDD” sends J.S. “a message on OfferUp or calls and says, ‘I want a Dyson or something.’” J.S. also stated that J.S. is “not sure exactly where,” but that J.S. “thinks he [“SIDD”] sells it [stolen new-in-box items]”.

11. J.S. advised that he believes that “SIDD” lives in Concord, North Carolina, and has met with “SIDD” in Concord, North Carolina and in southwest Charlotte, North Carolina, on numerous occasions, as many as “three days a week” to sell stolen items to “SIDD.” J.S. claimed to never have been to “SIDD’s” house, but “SIDD” often wanted to meet J.S. in Concord, North Carolina, to purchase stolen items from J.S. J.S. advised that “SIDD” drives a gold-colored Camry and a grayish-colored minivan. J.S. admitted that J.S. usually sells brand new-in-box stolen items to “SIDD” for approximately one-third of the item’s true retail price.

Surveillance of SIDDQUI, the PREMISES, and the VEHICLE

12. On or about March 11, 2020, another law enforcement officer drove by the PREMISES.³ The two-car garage door was open, and the officer observed that the garage was

³ According to law enforcement searches of law enforcement databases, including the North Carolina Division of Motor Vehicles, SIDDQUI resides at the PREMISES. This has been confirmed through multiple surveillances at the PREMISES by your Affiant and other law enforcement officers in which SIDDQUI was observed exiting and entering the PREMISES. Also according to the NC DMV, Rukshana PATEL (hereinafter “PATEL”) lives at the PREMISES. According to an internet-based home sales website, the PREMISES was last sold in approximately 2012; therefore, your Affiant believes that SIDDQUI has lived at the PREMISES since 2012.

almost completely filled with what appeared to be a large amount of retail store boxes, some of which were clearly observed to be DeWalt tool sets and Dyson vacuum cleaners.

13. On or about March 17, 2020, another law enforcement officer observed SIDDIQUI leave the PREMISES driving a 2008 silver Honda Odyssey, owned by SIDDIQUI, with North Carolina registration plate BBA9225, hereinafter “the VEHICLE,”⁴ remove what appeared to be two new-in-box retail store packages from the VEHICLE, and carry those packages inside the UPS Store located at 8611 Concord Mills Boulevard, Concord, North Carolina (hereinafter “the UPS STORE”).

14. On or about April 27, 2020, another law enforcement officer and your Affiant observed SIDDIQUI leave the PREMISES driving the VEHICLE and drive to the UPS STORE. SIDDIQUI removed what appeared to be approximately twelve new-in-box retail store packages from the VEHICLE and carried those packages inside the UPS STORE. SIDDIQUI left the UPS STORE empty-handed and then drove the VEHICLE back to the PREMISES.

15. Approximately one hour later on the same day, SIDDIQUI left the PREMISES in the VEHICLE and drove to a Kohl’s retail store parking lot located at 8875 Christenbury Parkway, Concord, North Carolina. Approximately several minutes after SIDDIQUI parked in the parking lot, a silver Volkswagen sedan driven by an individual later identified as J.S. parked next to the VEHICLE. SIDDIQUI opened the rear door of the VEHICLE and J.S. removed two SoClean 2 Automated CPAP Equipment Sanitizer Machines, hereinafter “the CLEANING MACHINES,” both of which were in retail store packages, from the Volkswagen and placed the CLEANING

⁴ According to the North Carolina Division of Motor Vehicles, SIDDIQUI owns the VEHICLE, which your Affiant and other law enforcement officers have observed parked in the driveway of the PREMISES on multiple dates.

MACHINES inside the VEHICLE. SIDDIQUI handed what appeared to be cash to J.S. who then counted the cash. J.S. immediately left the parking lot, and SIDDIQUI drove the VEHICLE back to the PREMISES. The transaction between J.S. and SIDDIQUI occurred within approximately one minute, and it appeared that J.S. and SIDDIQUI had at least met once before because there was almost no verbal communication between them during the transaction. When SIDDIQUI returned to the PREMISES, another law enforcement officer observed the contents of the PREMISES' garage when the garage door was open, and it appeared that the garage contained numerous new-in-box retail store packages similarly as observed on several previous dates.

16. Later on the same date, the EBAY STORE'S pre-existing advertisement for CLEANING MACHINES was changed by a person with access to the EBAY STORE. Your Affiant believes that the change made by the person with access to the EBAY STORE was to increase the quantity of CLEANING MACHINES available for sale as a result of SIDDIQUI purchasing two CLEANING MACHINES from J.S. earlier on this date.

17. On or about May 3, 2020, the EBAY STORE sold several CLEANING MACHINES for approximately \$265.00 with free shipping. An internet search revealed the retail price of new CLEANING MACHINES to be between approximately \$298.00 and \$348.00. This indicates to your Affiant that the EBAY STORE netted approximately \$210.00 for each CLEANING MACHINE after PayPal fees, eBay fees, and the cost of shipping were deducted from the sales price of the CLEANING MACHINES in the EBAY STORE.

18. On or about May 21, 2020, another law enforcement officer observed the VEHICLE parked in the PREMISES' driveway.

19. Retail store investigators at Target, The Home Depot, and Lowes provided your Affiant with retail and wholesale prices of items that are exclusively sold by their respective stores that were sold between approximately December 2019 and March 2020 by the EBAY STORE. Your Affiant compared the EBAY STORE's sales price and the EBAY STORE's net proceeds⁵ of each item to the retail and wholesale price of exclusive items⁶ sold by the retail stores. With very few exceptions, the EBAY STORE's sales price was between the retail and wholesale price of items, and the EBAY STORE's net proceeds of individual items was below or slightly above each item's wholesale price. Your Affiant knows that Target, The Home Depot, and Lowes are major retail stores in the United States whose respective wholesale purchase prices for items sold exclusively in their stores would be essentially impossible to profitably match through legal means. Therefore, there is probable cause to believe that the only way that the EBAY STORE's net proceeds of items could be comparable to the wholesale price of major U.S. retail stores is for the EBAY STORE's owner to purchase these items from persons who steal or fraudulently obtain the items and sell the stolen items at a severe drastic discount to the EBAY STORE's owner.

Paypal and Bank of America Accounts

20. During the course of the investigation, your Affiant has become aware of the following accounts linked to SIDDIQUI:

⁵ To summarize how eBay and Paypal are used, when a seller sells an item through eBay and receives payment via Paypal, the seller nets approximately 87% of the sales price of the item because the seller pays eBay a 10% fee and pays Paypal a 3% fee.

⁶ Many retail stores sell items that are "exclusive items," which means that only certain brands or certain models of products are available for purchase at particular retail stores. For instance, the brand "Dewalt" manufactures tools that are exclusively distributed to The Home Depot for retail sale to customers.

- a. Paypal Account XXXXXXXXXXXXXXXX5254, such account held in the name of “Shadab Siddiqui” (hereinafter “PAYPAL ACCOUNT”)
 - b. Bank of America Account XXXXXXXX0815, such account held in the name of “Rukshana A. Patel” (hereinafter “BANK OF AMERICA ACCOUNT 1”);
 - c. Bank of America Account XXXXXXXX7896, such account held in the names of “Shadab A. Siddiqui” and “Rukshana A. Patel” (hereinafter “BANK OF AMERICA ACCOUNT 2”); and
 - d. Bank of America Account XXXXXXXX4174, such account held in the name of “Rukshana A. Patel” (hereinafter “BANK OF AMERICA ACCOUNT 3”).
- (hereinafter, collectively, “the Funds”).

21. According to subpoenaed documents received by your Affiant from Paypal, SIDDQUI (named as “Shadab SIDDQUI” in Paypal documents) opened the PAYPAL ACCOUNT, in or about August 2005. The email address for the PAYPAL ACCOUNT is the EMAIL ACCOUNT, and the physical address for the PAYPAL ACCOUNT is the PREMISES.

22. According to subpoenaed information your Affiant received from Bank of America, BANK OF AMERICA ACCOUNT 1 is held in the name of “Rukshana A. PATEL,” and monthly bank statements are mailed to the PREMISES. BANK OF AMERICA ACCOUNT 2 is held in the names of “Shadab A. SIDDQUI” and “Rukshana A. PATEL,” and monthly bank statements are mailed to the PREMISES. BANK OF AMERICA ACCOUNT 3 is held in the name of “Rukshana A. PATEL,” and monthly bank statements are mailed to the PREMISES.

23. The PAYPAL ACCOUNT is linked to BANK OF AMERICA ACCOUNT 1 and BANK OF AMERICA ACCOUNT 2 which your Affiant knows allows SIDDIQUI, or anyone with access to the PAYPAL ACCOUNT, to transfer funds between the PAYPAL ACCOUNT, BANK OF AMERICA ACCOUNT 1, and BANK OF AMERICA ACCOUNT 2.

Funding of the Accounts

24. Between approximately October 2017 and March 2020, the PAYPAL ACCOUNT received approximately 1,500 individual payments totaling approximately \$330,000.00. The majority of the payments totaling approximately \$330,000.00 were from persons whose addresses are not in North Carolina and who bought items from the EBAY STORE. Between approximately October 2017 and March 2020, approximately \$280,000.00 was transferred from the PAYPAL ACCOUNT to BANK OF AMERICA ACCOUNT 1 and BANK OF AMERICA ACCOUNT 2.⁷ Further, during roughly this same time period, cash was withdrawn from BANK OF AMERICA ACCOUNT 1 and BANK OF AMERICA ACCOUNT 2. Your Affiant knows based on her training and experience that “fences” (individuals who buy and sell stolen property) often use cash to purchase such property from “boosters” (individual who steal property for

⁷ As to other sources of funding in the accounts, although SIDDIQUI appears to be employed by a legitimate business, it does not appear that SIDDIQUI has received deposits of income from his apparent legitimate employer in BANK OF AMERICA ACCOUNT 1, BANK OF AMERICA ACCOUNT 2 or BANK OF AMERICA ACCOUNT 3. However, PATEL is also legitimately employed and, between approximately September 2019 and December 2019, PATEL received an average monthly income from her apparent legitimate employer of approximately \$1,400.00 deposited into BANK OF AMERICA ACCOUNT 1. Nonetheless, according to BANK OF AMERICA ACCOUNT 1 statements, Patel has not received any monthly income from her employer since December 2019.

fences to sell). As of March 2020, the balance in the PAYPAL ACCOUNT was approximately \$2,848.75.

25. As to BANK OF AMERICA ACCOUNT 1 specifically, beginning in or about March 2019 and continuing at least through April 2020, funds from the PAYPAL ACCOUNT were deposited into BANK OF AMERICA ACCOUNT 1 in monthly aggregate amounts ranging between approximately \$9,000.00 and \$35,000.00. Beginning in or about March 2019 and continuing through April 2020, cash was withdrawn from Automated Teller Machines (ATMs) in Concord, North Carolina, near the PREMISES. The withdrawals were drawn on BANK OF AMERICA ACCOUNT 1 in monthly aggregate amounts ranging between approximately \$1,200.00 and \$4,000.00. As of late March 2020, there was a balance of approximately \$7,800.00 in BANK OF AMERICA ACCOUNT 1.

26. As to BANK OF AMERICA ACCOUNT 2, beginning in or about March 2019 and continuing at least through December 2019, funds from the PAYPAL ACCOUNT were deposited into BANK OF AMERICA ACCOUNT 2 in monthly aggregate amounts ranging between approximately \$2,000.00 and \$15,000.00. Beginning in or about March 2019 and continuing through December 2019, cash was withdrawn from ATMs in Concord, North Carolina near the PREMISES from BANK OF AMERICA ACCOUNT 2 in monthly aggregate amounts ranging between approximately \$2,000.00 and \$7,000.00. On or about January 17, 2020, approximately \$3,000.00 was withdrawn from BANK OF AMERICA ACCOUNT 2 and on or about January 22, 2020, approximately \$8,000.00 was deposited from the PAYPAL ACCOUNT into BANK OF AMERICA ACCOUNT 2. As of late March 2020, there was a balance of approximately \$4,500.00 in BANK OF AMERICA ACCOUNT 2.

27. As to BANK OF AMERICA ACCOUNT 3, beginning in or about June 2019 and continuing through April 2020, BANK OF AMERICA ACCOUNT 3 received deposits from BANK OF AMERICA ACCOUNT 1 and BANK OF AMERICA ACCOUNT 2 in monthly aggregate amounts ranging between approximately \$2,000.00 and \$35,000.00. During this same time period, there were very few transactions other than deposits from BANK OF AMERICA ACCOUNT 1 and BANK OF AMERICA ACCOUNT 2 into BANK OF AMERICA ACCOUNT 3. Based on this pattern of conduct, one or more conspirators appear to use BANK OF AMERICA ACCOUNT 3 as a repository account into which funds from BANK OF AMERICA ACCOUNT 1 and BANK OF AMERICA ACCOUNT 2 are deposited. In total, BANK OF AMERICA ACCOUNT 3 received approximately \$210,000.00 from BANK OF AMERICA ACCOUNT 1 and BANK OF AMERICA ACCOUNT 2 between approximately June 2019 and April 2020. As of April 2020, there was a balance of approximately \$180,000.00 in BANK OF AMERICA ACCOUNT 3.

BACKGROUND CONCERNING EMAIL

28. In general, an email that is sent to a Google subscriber is stored in the subscriber's "mail box" on Google servers until the subscriber deletes the email. If the subscriber does not delete the message, the message can remain on Google servers indefinitely. Even if the subscriber deletes the email, it may continue to be available on Google's servers for a certain period of time.

29. In my training and experience, I have learned that GOOGLE provides a variety of on-line services, including electronic mail ("email") access, to the public. GOOGLE allows subscribers to obtain email accounts at the domain name gmail.com, like the email account listed in Attachment A. Subscribers obtain an account by registering with GOOGLE. During the

registration process, GOOGLE asks subscribers to provide basic personal information. Therefore, the computers of GOOGLE are likely to contain stored electronic communications (including retrieved and unretrieved email for GOOGLE subscribers) and information concerning subscribers and their use of GOOGLE services, such as account access information, email transaction information, and account application information. In my training and experience, such information may constitute evidence of the crimes under investigation because the information can be used to identify the account's user or users.

30. A GOOGLE subscriber can also store with the provider files in addition to emails, such as address books, contact or buddy lists, calendar data, pictures (other than ones attached to emails), and other files, on servers maintained and/or owned by GOOGLE. In my training and experience, evidence of who was using an email account may be found in address books, contact or buddy lists, email in the account, and attachments to emails, including pictures and files.

31. In my training and experience, email providers generally ask their subscribers to provide certain personal identifying information when registering for an email account. Such information can include the subscriber's full name, physical address, telephone numbers and other identifiers, alternative email addresses, and, for paying subscribers, means and source of payment (including any credit or bank account number). In my training and experience, such information may constitute evidence of the crimes under investigation because the information can be used to identify the account's user or users. Based on my training and my experience, I know that, even if subscribers insert false information to conceal their identity, this information often provides clues to their identity, location, or illicit activities.

32. In my training and experience, email providers typically retain certain transactional information about the creation and use of each account on their systems. This information can include the date on which the account was created, the length of service, records of log-in (*i.e.*, session) times and durations, the types of service utilized, the status of the account (including whether the account is inactive or closed), the methods used to connect to the account (such as logging into the account via the provider's website), and other log files that reflect usage of the account. In addition, email providers often have records of the Internet Protocol address ("IP address") used to register the account and the IP addresses associated with particular logins to the account. Because every device that connects to the Internet must use an IP address, IP address information can help to identify which computers or other devices were used to access the email account.

33. In my training and experience, in some cases, email account users will communicate directly with an email service provider about issues relating to the account, such as technical problems, billing inquiries, or complaints from other users. Email providers typically retain records about such communications, including records of contacts between the user and the provider's support services, as well as records of any actions taken by the provider or user as a result of the communications. In my training and experience, such information may constitute evidence of the crimes under investigation because the information can be used to identify the account's user or users.

34. As explained herein, information stored in connection with an email account may provide crucial evidence of the "who, what, why, when, where, and how" of the criminal conduct under investigation, thus enabling the United States to establish and prove each element or alternatively, to exclude the innocent from further suspicion. In my training and experience, the

information stored in connection with an email account can indicate who has used or controlled the account. This “user attribution” evidence is analogous to the search for “indicia of occupancy” while executing a search warrant at a residence. For example, email communications, contacts lists, and images sent (and the data associated with the foregoing, such as date and time) may indicate who used or controlled the account at a relevant time. Further, information maintained by the email provider can show how and when the account was accessed or used. For example, as described below, email providers typically log the Internet Protocol (IP) addresses from which users access the email account, along with the time and date of that access. By determining the physical location associated with the logged IP addresses, investigators can understand the chronological and geographic context of the email account access and use relating to the crime under investigation. This geographic and timeline information may tend to either inculcate or exculpate the account owner. Additionally, information stored at the user’s account may further indicate the geographic location of the account user at a particular time (*e.g.*, location information integrated into an image or video sent via email). Last, stored electronic data may provide relevant insight into the email account owner’s state of mind as it relates to the offense under investigation. For example, information in the email account may indicate the owner’s motive and intent to commit a crime (*e.g.*, communications relating to the crime), or consciousness of guilt (*e.g.*, deleting communications in an effort to conceal them from law enforcement).

CONCLUSION

35. Based on the forgoing, I request that the Court issue the proposed Warrant.

36. Pursuant to 18 U.S.C. § 2703(g), the presence of a law enforcement officer is not required for the service or execution of this Warrant. The government will execute this Warrant

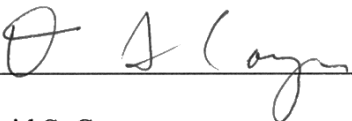
by serving the Warrant on GOOGLE. Because the Warrant will be served on GOOGLE, who will then compile the requested records at a time convenient to it, reasonable cause exists to permit the execution of the requested Warrant at any time in the day or night.


Respectfully submitted,

/s/ Brittany M. Wright

Brittany M. Wright
Special Agent
United States Secret Service

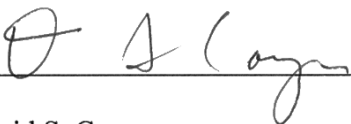
Signed: May 26, 2020




David S. Cayer
United States Magistrate Judge

United States Magistrate Judge

In accordance with Rule 4.1(b)(2)(A), the Affiant attested under oath to the contents of this Affidavit, which was submitted to me by reliable electronic means, on this __26th__ day of May, 2020, at __2:05 pm____.

Signed: May 26, 2020



David S. Cayer
United States Magistrate Judge


ATTACHMENT A

Property to Be Searched

This warrant applies to information associated with **shadab.siddiqui@gmail.com** that is stored at premises owned, maintained, controlled, or operated by Google, a company headquartered in Mountain View, California.

ATTACHMENT B

Particular Things to be Seized

I. Information to be disclosed by Google] (the “Provider”)

To the extent that the information described in Attachment A is within the possession, custody, or control of the Provider, regardless of whether such information is located within or outside of the United States, and including any emails, records, files, logs, or information that has been deleted but is still available to the Provider, the Provider is required to disclose the following information to the government for each account or identifier listed in Attachment A:

- a. The contents of all emails associated with the account from January 1, 2019 through the present, including stored or preserved copies of emails sent to and from the account, draft emails, the source and destination addresses associated with each email, the date and time at which each email was sent, and the size and length of each email;
- b. All records or other information regarding the identification of the account, to include full name, physical address, telephone numbers and other identifiers, records of session times and durations, the date on which the account was created, the length of service, the IP address used to register the account, log-in IP addresses associated with session times and dates, account status, alternative email addresses provided during registration, methods of connecting, log files, and means and source of payment (including any credit or bank account number);
- c. The types of service utilized;
- d. All records or other information stored by an individual using the account, including address books, contact and buddy lists, calendar data, pictures, and files; and
- e. All records pertaining to communications between the Provider and any person regarding the account, including contacts with support services and records of actions taken.

The Provider is hereby ordered to disclose the above information to the government within 14 days of issuance of this warrant.

II. Information to be seized by the government

All information described above in Section I that constitutes fruits, contraband, evidence, and instrumentalities of violations of 18 U.S.C. § 2314 (Interstate Transportation of Stolen Property), 18 U.S.C. § 371 (Conspiracy), and 18 U.S.C. §§ 1956 and 1957 (Money Laundering), those violations involving **SIDDIQUI** and occurring after January 1, 2019, including, for each account or identifier listed on Attachment A, information pertaining to the following matters:

- (a) Evidence associated with the purchase or sale of brand new retail store items, including purchase or sale receipts and communication with persons or companies regarding the purchase or sale of brand new retail store items.
- (b) Evidence indicating how and when the email account was accessed or used, to determine the geographic and chronological context of account access, use, and events relating to the crime under investigation and to the email account owner;
- (c) Evidence indicating the email account owner's state of mind as it relates to the crime under investigation;
- (d) The identity of the person(s) who created or used the user ID, including records that help reveal the whereabouts of such person(s).